REMINDERS FOR EMPLOYEES

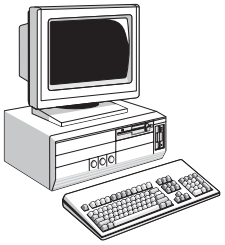
UNLICENSED SOFTWARE: Not to be installed on any CDSS system.

PASSWORDS: Passwords are confidential and must not be shared except with the supervisor or his/her designee. Passwords must be changed every 60 days.

PRIVACY: Inform the employee that Internet/E-Mail usage is not private and is not personal property. The Department reserves the right to monitor computer usage without prior notice. Suspected violation of the policy may be investigated without notice.

INFORMATION SECURITY PAMPHLETS:
In addition to providing the employee with all information policies, the following pamphlets have been developed by the Information Security and Management Systems Branch for employees. These summarize key policy provisions:

- Good Information Security Practices (PUB 304)
- Protecting Confidential or Sensitive Information (PUB 311)
- Reporting Incidents (PUB 312)



PERSONAL COMPUTER ADMINISTRATOR (PCA) PROVIDED ORIENTATION: Instruct the PCA/designee to discuss any additional requirements and security practices used in the organization.

EXEMPTION REQUESTS: Exemption requests for Information Security (GEN 1313) must be submitted to and approved by the Information Security Officer. Questions may be referred to the Information Security and Management Systems Branch at (916) 657-3409.

☑ FOR EXITING EMPLOYEE

Supervisors are responsible for ensuring that the following actions are taken when an employee leaves the organization:

- ☐ Employee must return all confidential/ sensitive data.
- ☐ Employee must return access and charge cards, etc.
- ☐ Terminate PC access permissions within one day after departure (GEN 1321).
- ☐ PCA or Supervisor must inspect the PC, laptop, or personal digital assistant.
- ☐ Complete GEN 1322 (Employee Transfer Notice) or PS 381 (Employee Separation Notice).
- ☐ Forms requiring employee signature, include GEN 1321, and either GEN 1322 or PS 381.

For Completion by Supervisor:

ARRIVAL IN UNIT:

EMPLOYEE NAME: _____

DATE:

SEPARATION FROM UNIT:

EMPLOYEE NAME: _____

DATE:

State of California
Gray Davis, Governor
Health and Human Services Agency
Grantland Johnson, Secretary
Department of Social Services
Rita Saenz, Director
PUB 345 (6/00)

SUPERVISOR'S INFORMATION SECURITY

☑ Checklist

FOR EMPLOYEES

Supervisors can use this checklist for an employee orientation or exit to ensure that an employee is advised of the CDSS Information Security (IS) policies and/or appropriate action is taken to initiate/terminate computer access. This form can also be used for consultants, contractors, vendors, volunteers, etc.
Any questions or clarification of policies or practices may be directed to the Information Security and Management Systems Branch (ISMSB) at
(916) 657-3409.

FOR NEW EMPLOYEE

Supervisors should provide the following information to all employees:

- ☐ All information security policies.
- ☐ Identify confidential and sensitive information for the organization and how to protect it (see policy).
- ☐ Internet/E-Mail usage and E-Mail retention periods (90 days).
- ☐ Vendor confidentiality requirements.
- ☐ Record retention schedules.
- ☐ Back-up procedures and schedules.
- ☐ Explanation of password requirements and protections. (Changed every 60 days).
- ☐ Explanation of procedures for reporting incidents (example: suspected virus).
- ☐ Explanation that there is no expectation of privacy in the use of the Internet/E-Mail.
- ☐ Explanation of which system access/permissions are granted (use the GEN 1321).
- ☐ Have the Personal Computer Administrator (PCA) or designee provide PC orientation.
- ☐ Forms requiring employee signature:
  - (1) Internet/E-Mail Usage Policy
  - (2) E-Mail Retention Policy
  - (3) Access Policy

INFORMATION SECURITY POLICIES

Information Security (IS) policies are available from the CDSS Homepage at
http://sac8.dss.ca.gov/ISO/toc02.htm
You may also contact the Information Security and Management Systems Branch at
(916) 657-3409.

Provide the following policies to <u>all</u> staff:

1. IS Roles and Responsibilities Policy.
2. E-Mail Retention Policy.
3. Internet and E-Mail Usage Policy.
4. Policy for Security of Confidential and Sensitive Data.
5. Guidelines for Destruction of Confidential and Sensitive Information.
6. Guidelines for Protection of Confidential and Sensitive Information.
7. Back-Up Policy.
8. Guidelines for Identifying Necessary Data.
9. Employee Password Control Policy/Guidelines for Password Protection and Security.
10. Virus Protection.
11. Incident Policy.
12. Laptop Security Policy.
13. Employee Separation and Transfer Policy.
14. Policy for the Review of Information Security Related Documents.
15. Personal Computer Security Policy.
16. Access Control Policy.

Additional Policies for PCA/System Administrators

1. Guidelines for Establishing a Back-Up Process.
2. Guidelines for Choosing a Back-Up Process.
3. Personal Computer Administrator Password Controls Policy.
4. System Administrator Password Control Policy.
5. Password Controls Policy Implementation Plan.
6. System and Application Access form (GEN 1321).
7. Incident Report form (GEN 1311).

SUPERVISORS ARE RESPONSIBLE FOR:

SYSTEM/APPLICATION ACCESS . . . authorizing user ID and system access permissions and informing the employee of the access permissions granted. Use GEN 1321 System Access Authorization Form for this purpose.

IS POLICIES . . . providing employees with all CDSS IS policies and informing the employees of their responsibility to read and work in accordance with them.

CONFIDENTIAL AND SENSITIVE INFORMATION . . . explaining the classification (confidential, sensitive, etc.) of the data and documents for which the employee will be responsible.

DISPOSAL/DESTRUCTION PROCEDURES . . . explaining disposal/destruction procedures to be followed.

BACK-UPS . . . explaining system back-up procedures and schedules for the organization.

VIRUS PROTECTION . . . explaining that virus protection software is not to be deactivated; discontinue the use of the PC and report any suspected virus promptly; scan any diskettes for virus infection prior to using in CDSS computers; extend license for virus protection software to home computer if needed.

INCIDENT REPORTS . . . informing employee to whom they should report information security incidents (i.e., an event, intentional or unintentional that causes the loss, damage to, destruction, or unauthorized disclosure of CDSS information assets, or mis-use of our systems and network).

DOCUMENT REVIEW . . . ensuring that necessary documents are reviewed and approved by the Information Security Officer (See Policy for the Review of Information Security Related Documents).